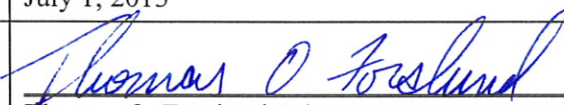


Thomas O. Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Breach Notification
<b>Policy Number:</b>	AS-021
<b>Effective Date:</b>	July 1, 2013
<b>Approval:</b>	 Thomas O. Forslund, Director
	6/17/13 Date

**Purpose:**

This policy establishes Wyoming Department of Health's (WDH) framework for addressing a breach of unsecured protected health information (PHI) that occurs notwithstanding WDH's recognition of the importance of information security and its reasonable efforts to prevent such a breach.

**Scope:**

This policy applies to all WDH workforce members.

**Definitions:**

*Access* means the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

*Breach* means the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the by the Privacy Rule which compromises the security or privacy of such information. (For exceptions to the definition of breach, please consult 45 CFR § 164.402.)

*Discovered* means the first day on which the breach is known or would have been known to a WDH workforce member by exercising reasonable diligence.

*Incident* means an impermissible acquisition, access, use, or disclosure of PHI.

*Law enforcement official* means an officer or employee of any agency or authority of the United States, a state or territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

*Protected health information (PHI)* generally means identifiable or potentially identifiable health information that is transmitted or maintained in electronic media or any other form or medium. (For the complete definition, please consult 45 CFR § 160.103).

*Unsecured protected health information* means PHI that is not secured through the use of a technology or methodology specified by the Secretary that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

**Policy:**

- 1. General.** WDH shall outline its process for evaluating and reporting known or suspected privacy violations or security incidents. This process shall include a contact list (WDH Form SF-006; Incident Contact List) indicating to whom reports of such incidents should be made; who should be involved in determining if a breach of unsecured PHI has occurred; and if affected individual(s) should be notified.
- 2. Reporting incidents and complaints**
  - a. WDH workforce members shall immediately report known or suspected privacy violations or security incidents to the WDH Compliance Office in accordance with WDH Policy AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents.
  - b. As soon as possible, but not later than forty-five (45) calendar days following discovery of an incident, the WDH Compliance Office shall complete a risk assessment to determine the probability that PHI has been compromised and attach it to the report,. The risk assessment shall include:
    - i. The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification.
      - A. Was PHI involved;
      - B. Type of PHI;
      - C. Does the incident meet the definition of breach; and
      - D. Likelihood of re-identification.
    - ii. The person who used the PHI or to whom the disclosure was made.
      - A. Did the recipient have an obligation to protect the privacy and security of PHI;
      - B. Was the acquisition, access, or use of PHI by a workforce member or person acting under the authority of WDH;
      - C. Was such acquisition, access, or use made in good faith;
      - D. Does the recipient have the ability to re-identify the PHI;
      - E. Was the acquisition, access, or use within the recipient's scope of authority; and
      - F. Did the acquisition, access, use, or disclosure result in further use or disclosure in a manner not permitted by the Privacy Rule.
    - iii. A determination of whether the PHI was actually acquired or viewed, or rather, the opportunity to acquire or view existed, but was not acted upon.
      - A. Was the PHI encrypted using at least 128 bit encryption or destroyed by an acceptable method of destruction;
      - B. Following a forensic examination, did evidence establish that the information was not accessed.
    - iv. The extent to which the risk to the PHI has been mitigated.
      - A. A satisfactory assurance has been received from the recipient stating that the PHI has or will not be further used or disclosed.
      - B. The efficiency of the mitigation effectively limited availability to the PHI;
      - C. Does an exception to the notification requirement exist; and
      - D. Do the affected individuals need to be notified.
  - c. Answers to the questions listed above may not always be available.
- 3. Review by the designated Attorney General's representative**
  - a. If, after reviewing the risk assessment and making an initial evaluation, the WDH Compliance Office determines that a breach of unsecured PHI may have occurred, the WDH Compliance Office shall refer the event to the designated Attorney General's representative to assist in making the final determination of whether a breach of unsecured PHI has occurred. If, through an independent risk assessment, the designated Attorney General's

- representative determines that a breach of unsecured PHI has occurred, the designated Attorney General's representative shall recommend notification and assist the WDH Compliance Office in determining whether the breach requires a press release.
- b. If a press release is required, the WDH Compliance Office shall consult with the WDH Public Information Officer.
4. **Evaluating an incident or complaint.** The reporting obligation for WDH is triggered when a breach of unsecured PHI occurs. In order to have a breach of unsecured PHI, there must be **PHI + a violation of the HIPAA Privacy Rule + compromise of the privacy and security of the PHI + unsecured PHI + no exceptions**. Sections 4.a.-c. Below may be utilized to accurately evaluate a privacy incident or complaint.
- a. PHI involved. If no PHI is involved, there is no breach of unsecured PHI and no obligation to notify.
  - b. Violation of the Privacy Rule. If the WDH Compliance Office determines that the violation compromises the privacy and the security of PHI, then the violation is a "breach."
  - c. Ability of WDH to mitigate the risk of harm. The risk of harm may depend upon the ability of WDH to mitigate the effects of the breach.
5. **Securing PHI through encryption or destruction.** WDH shall utilize one of the two following methods for "securing" PHI:
- a. Encryption. WDH shall encrypt PHI using a NIST recommended algorithm and procedure. To comply with encryption standards and ensure the encryption keys are not obtained, WDH shall keep encryption keys on a separate device.
  - b. Destruction. Paper, film, or other hard copy media shall be shredded or destroyed in a manner that the PHI cannot be read or otherwise reconstructed.
6. **Law enforcement notification delay.** WDH may delay its notification to affected individuals for a criminal investigation or for national security purposes.
- a. If a law enforcement official informs WDH that notice to an individual, to the Secretary of the U.S. Department of Health and Human Services (DHHS), or to the media would impede a criminal investigation or cause damage to national security, WDH shall request that the law enforcement official make an official written request that WDH delay such notification. The written request shall include:
    - i. The law enforcement official's full name;
    - ii. The law enforcement official's title and badge number;
    - iii. The law enforcement organization's name;
    - iv. The reason for the delay; and
    - v. The proposed number of days to delay.
  - b. All oral requests for a notification delay shall be evaluated on a case by case basis and only granted in the most urgent and serious circumstances. If WDH receives an oral request, such request shall be documented.
7. **Notification**
- a. If the WDH Compliance Office determines a breach of unsecured PHI has occurred, the WDH shall provide notice of the breach and maintain documentation of such notice.
  - b. Notice to the affected individual(s). Unless contrary instructions from law enforcement are received, a written notice of breach shall be provided to each affected individual whose unsecured PHI has been breached, or is reasonably believed to have been breached, as follows:

- i. Timing of notice. The notice shall be provided no later than sixty (60) calendar days after WDH discovers the breach. The breach is considered “discovered” on the first day a WDH workforce member or agent knows, or by exercising reasonable diligence, would have known, of the breach.
  - ii. Manner of notice. The written notice shall be:
    - A. Sent by first-class mail addressed to the affected individual’s last known address;
      - I. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn;
    - B. Provided to the individual’s personal representative, if the individual is deceased, and if WDH has the personal representative’s address; or
    - C. Provided in one or more mailings as additional information becomes available.
  - iii. Content of notice. The notice shall be written in plain language and shall contain the following information:
    - A. A brief description of the incident, including the date of the breach and the date of the discovery of the breach, if known;
    - B. A description of the types of unsecured PHI involved in the breach;
    - C. Any steps the individual should take to protect him or herself from harm that could result from the breach;
    - D. A brief description of the steps WDH is taking to investigate the breach, to mitigate the harm to the individual, and to protect against future occurrences; and
    - E. Contact information, including a toll-free telephone number, an e-mail address, website, or postal address for the individual to ask questions or learn additional information.
  - iv. Substitute notice. If insufficient or out-of-date contact information for an individual precludes written notice to such individual, the WDH shall provide notice reasonably calculated to reach the individual as soon as reasonably possible after such determination, as described below.
    - A. If there is insufficient or out-of-date contact information for fewer than ten (10) individuals, notice may be provided by e-mail, telephone, or other means.
    - B. If there is insufficient or out-of-date contact information for ten (10) or more individuals, notice shall:
      - I. Be in the form of either a conspicuous posting for ninety (90) calendar days on the WDH Internet home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside; and
      - II. Include a toll-free number that remains active for at least ninety (90) calendar days so that the individual can learn whether his or her unsecured PHI was included in the breach.
    - C. Substitute notice need not be provided if the affected individual is deceased and the WDH has insufficient or out-of-date contact information for the next of kin or personal representative of the individual.
  - v. Urgent notice. If WDH determines that potential for imminent misuse of the unsecured PHI in connection with a breach exists, WDH may provide information regarding the breach to individuals by telephone or other means, as appropriate, in addition to providing the required written notice as described above.
- c. Notice to DHHS. Unless contrary instructions from law enforcement are received, WDH shall notify DHHS of the breach of unsecured PHI. Such notification shall be provided as follows:
- i. If the breach involves 500 or more individuals, WDH shall notify DHHS in a manner specified by DHHS on its website of the breach contemporaneously with providing the notice to the individual.

- ii. If the breach involves less than 500 individuals, the WDH shall maintain a log or similar documentation of the breach of unsecured PHI and shall report the information specified by DHHS on its website no later than February 28<sup>th</sup> of the following year.
- d. Notice to media. Unless contrary instructions from law enforcement are received, and a breach involves more than 500 residents of one state or jurisdiction, the WDH shall notify prominent media outlets serving the state or jurisdiction in addition to notifying the individual and DHHS. Such notice shall be provided no later than sixty (60) calendar days after discovery of the breach. The notice shall contain the same information included in the notice to the individual.
- e. Communications with the media or outside agencies. With the exception of the WDH Compliance Office, Public Information Officer, or designee, WDH workforce members are not authorized to speak on behalf of WDH to media personnel or representatives of other outside agencies concerning a breach.
- f. Retention of breach notice documentation. The WDH shall record and maintain thorough records of all activities related to breaches of unsecured PHI, the provision of notice to individuals, DHHS, or the media, and communications from law enforcement related to delayed notification, if applicable, for at least six (6) years from the date the incident was closed or notice was provided, whichever date is the latest.
- g. Reporting of incidents to WDH by its business associates
  - i. In the event of a breach of unsecured PHI, a WDH business associate (BA) is required to:
    - A. Notify WDH no later than seven (7) business days following discovery of an incident involving WDH's PHI. The BA shall provide to the WDH Compliance Office the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been breached and any other available information that WDH is required to provide to the individual for further processing in accordance with this policy.
    - B. Complete a risk assessment no later than seven (7) business days following discovery of an incident involving WDH's PHI to determine whether there has in fact been a breach. If definite answers to all of the questions above are not available at the time the incident is reported, the BA shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from a breach is on WDH - not the BA. Therefore, a BA should not have the discretion to determine whether notification will occur.
  - ii. WDH shall:
    - A. Include appropriate language in all contracts with BAs to reflect the BA's responsibilities.
    - B. Consult with the designated Attorney General's representative when an incident is reported by a BA, to determine whether notification is required.



**Contacts:**

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

**Forms:**

SF-006; Incident Contact List

**Policies:**

AS-007; De-identification and Re-identification of PHI; Limited Data Sets and Data Use Agreements  
AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents

**References:**

45 CFR 164 Subpart D  
NIST SP-800-111, Guide to Storage Encryption Technologies for End User Devices  
NIST SP-800-88, Guidelines for Media Sanitization

**Training:**